

(12) UK Patent Application (19) GB (11) 2 355 892 (13) A

(43) Date of A Publication 02.05.2001

(21) Application No 0018673.4

(22) Date of Filing 31.07.2000

(30) Priority Data

(31) 9909966

(32) 30.07.1999

(33) FR

(51) INT CL⁷
H04Q 7/32

(52) UK CL (Edition S)
H4L LEF L209

(56) Documents Cited
GB 2335568 A
WO 97/43866 A2

GB 2285559 A EP 0607767 A1

(71) Applicant(s)

Sagem SA

(Incorporated in France)

6 Avenue d'Iena, 75116 Paris, France

(58) Field of Search
UK CL (Edition S) H4L LEF
INT CL⁷ H04Q 7/32 7/38
Online Databases: WPI, EPODOC, JAPIO

(72) Inventor(s)

Yves Portalier

Christine Licens

Jean-Marc Dimech

Frederic Dupas

(74) Agent and/or Address for Service

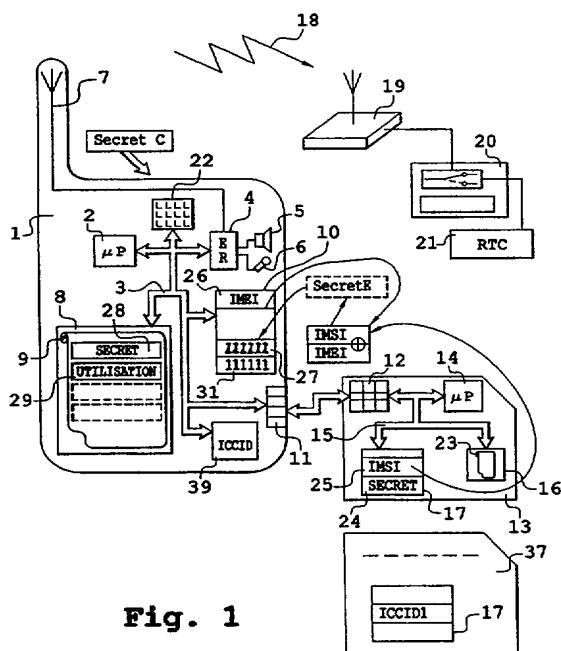
Fitzpatricks

39 Stukeley Street, LONDON, WC2B 5LT,
United Kingdom

(54) Abstract Title

Method for putting a mobile telephone into service

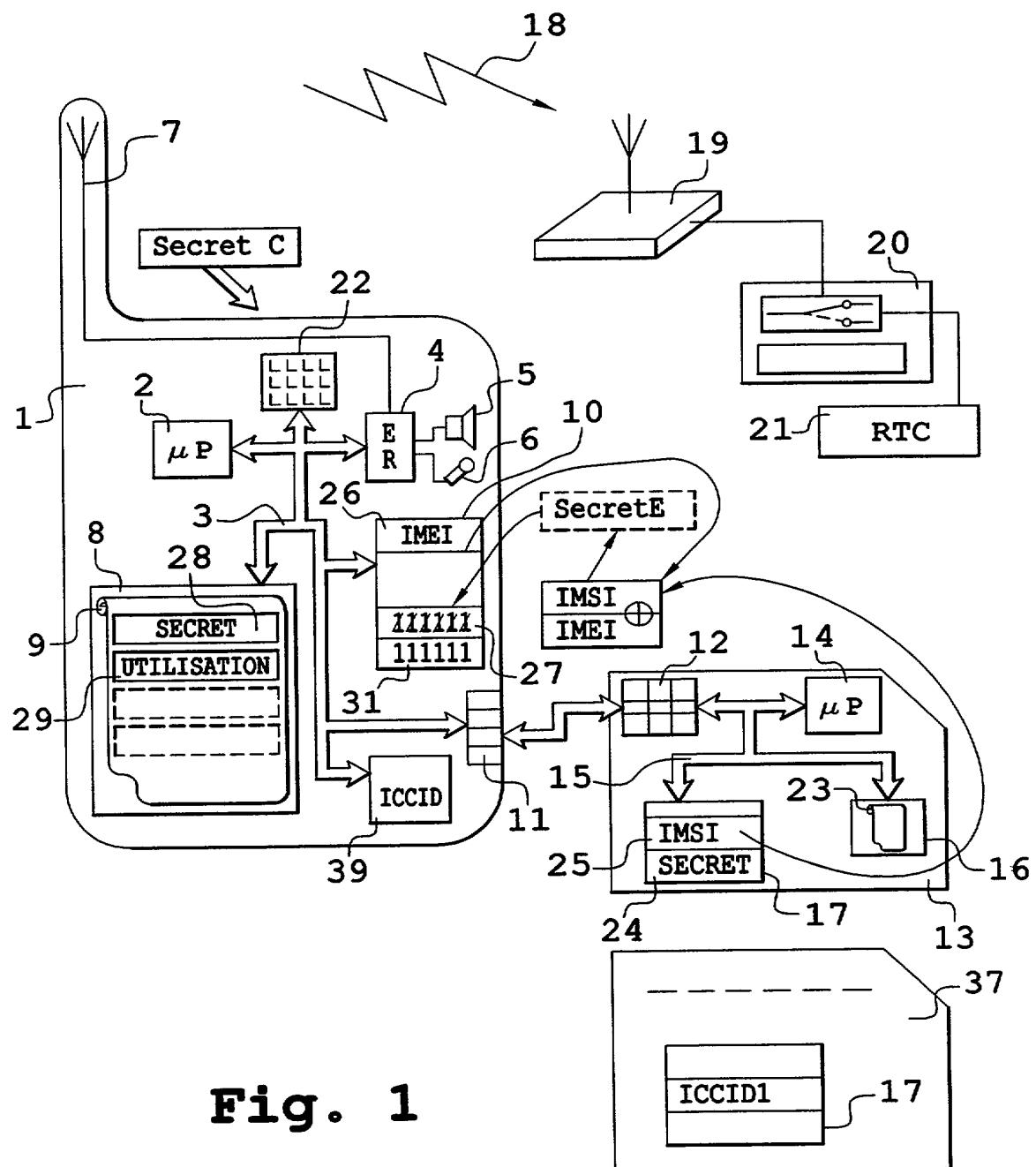
(57) A mobile telephone 1 has a first SIM (subscriber identity module) 13 which stores an IMSI code. The IMSI code is also stored in the memory of the phone in encrypted form. The mobile phone can only be put into service when a comparison of the two codes is successful. A PIN code may also need to be keyed in. To allow a genuine owner to use a second SIM, he can key in a secret unit code when the comparison of IMSI codes fails. This secret unit code is compared to a unit code stored in the mobile and if successful, the IMSI code of the second SIM replaces that of the first SIM in the memory of the mobile phone. For first time operation the IMSI code in the mobile phone is pre-recorded as binary 1's before it is personalised to the IMSI of the SIM.. If the owner forgets his secret unit code, a special removable circuit 37 replacing the SIM can be used by the network operator to reveal the unit code on the mobile phone display.



At least one drawing originally filed was informal and the print reproduced here is taken from a later filed formal copy.

This print takes account of replacement documents submitted after the date of filing to enable the application to comply with the formal requirements of the Patents Rules 1995

GB 2 355 892 A

**Fig. 1**

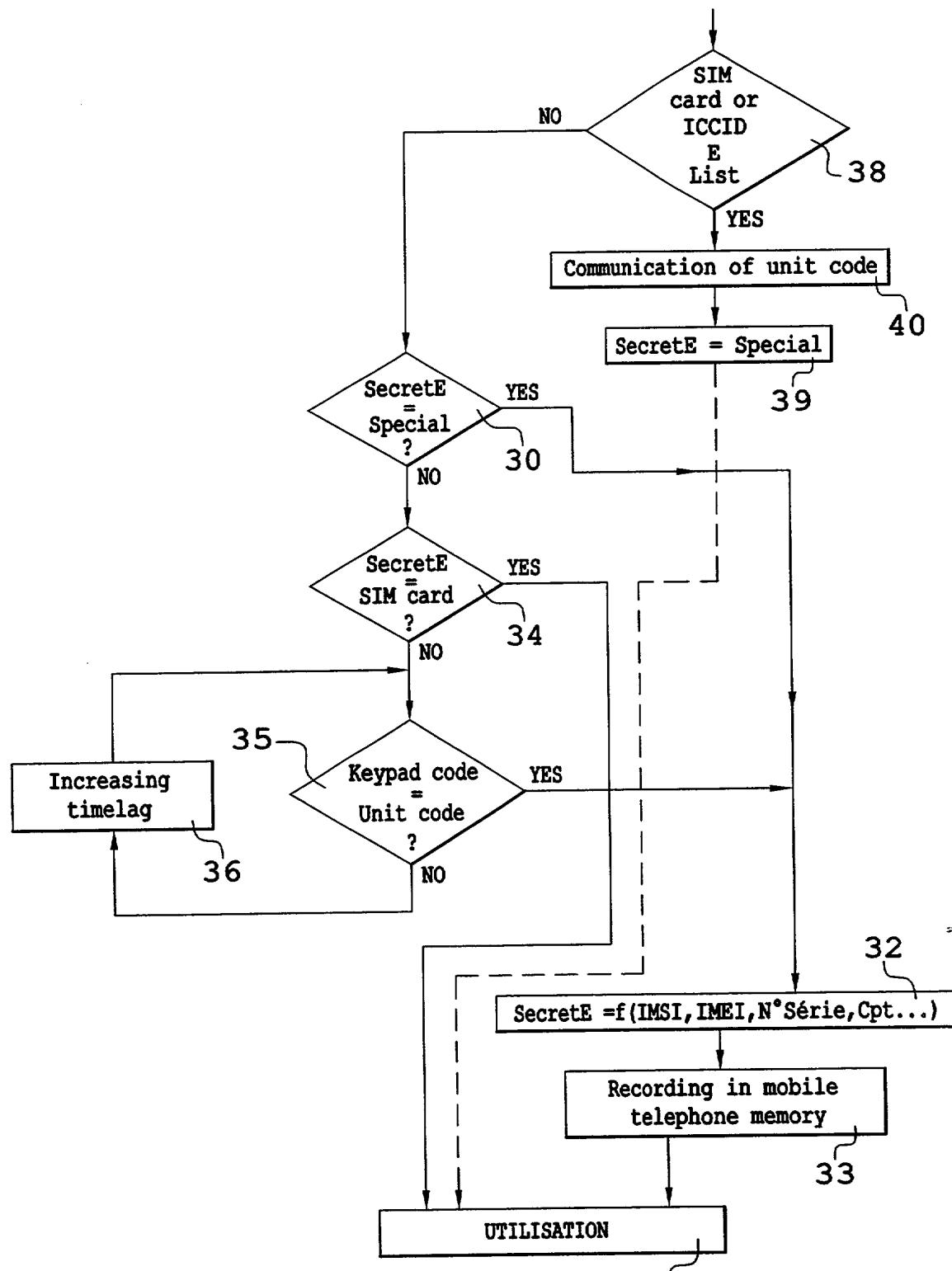


Fig. 2

METHOD FOR PUTTING A MOBILE TELEPHONE INTO SERVICE

An object of the present invention is a method for putting a mobile telephone into service. The aim of the invention is to prevent theft or, at least, to prevent thieves from feeling any temptation whatsoever to steal a mobile telephone.

In mobile telephony, it is known, especially in the field of GSM applications, that a mobile telephone is associated with a removable security circuit known as a SIM (Secure Identification Module). A secure identification circuit of this kind has two main functions. Firstly, and essentially for an operator who places a circuit of this kind at the disposal of the mobile telephone owner, this circuit contains information on this operator. This information is represented by an IMSI (International Mobile Subscriber Identity) code stored in a SIM. This information pertains to a subscription contract, consisting in practice of frequency bands allocated by a regulating authority to this operator, and a telephone number given to the user so that he can receive calls from outside.

Secondly, by way of additional functions, it has been proposed that this use of the subscription should itself be secured through the keying in, on the keypad of the mobile telephone, of a code known as a PIN or Personal Identification Number. This keying-in operation is designed to enable a processing operation, preferably inside the SIM circuit, of the PIN code keyed in by the user and the comparison of this PIN code thus processed with a secret code contained in the secured SIM circuit. Thus, the secured SIM circuit also has an undetectable, inviolable, secret code and a processing algorithm to compare the keyed-in PIN code with this inviolable code. This keyed-in PIN code and the secret code of the SIM circuit should not be mistaken for the subscriber information which too is present in the form of the IMSI code.

In practice, a system of this kind works well. Indeed, since the removable SIM circuit is placed permanently inside the mobile telephone, anyone who steals a mobile telephone must key in the PIN code, which he does not know, when he tries to put this telephone into service. Thus, he cannot use the mobile telephone whose true owner can soon cancel his subscription.

However, a device of this kind has the drawback wherein it is the

subscription that is protected far more than the mobile telephone itself. Indeed, since the sums corresponding to the use of the telephone generated in a subscription may be very high and may exceed the cost of the mobile telephone itself, it is above all this use of the telephone that has been
5 protected. This approach means, however, that anyone taking out a subscription with a mobile telephony operator only has to ask this operator for a SIM circuit that is specific to this operator and gives concrete form to his subscription. With a new SIM circuit of this kind replacing a previous SIM card, a thief can use a stolen mobile telephone.

10 In theory, this should not happen since mobile telephones themselves have an identification, an IMEI – International Mobile Equipment Identity – code. This IMEI code is not a secret. A sequence of keys on the mobile telephone reveals this code on the screen of the telephone. Whenever any calls are exchanged with a mobile telephone of this kind, this IMEI code is
15 normally transmitted to an operator. Therefore it should be possible, since the IMEI code of a stolen mobile telephone is known, to warn every operator that this telephone should no longer be used. In practice, the diversity of the operators, even in one and the same national region, means that this data which provides information on the user of a stolen telephone is not managed
20 in such a way as to obtain the restitution of the mobile telephone, or at least in such a way as to prevent theft.

The aim of the invention is to provide an efficient remedy to this problem of theft. In the invention, the aim has been to ensure that when a mobile telephone is stolen, it is not only the subscription but also the mobile
25 telephone that is no longer usable. Therefore it is proposed to duplicate all or part of the IMSI code (or even another code) of the SIM security circuit in the memory of the mobile telephone, in the form of a copy but preferably in an encrypted way. Consequently, the IMSI code will be present twice, each time in clear or non-encrypted form and in an encrypted form. It will be present in
30 the SIM circuit, as in the prior art, and it will be present in the memory of the mobile telephone. When the mobile telephone is put into service, a comparison is then prompted in a starting algorithm of the mobile telephone to ascertain that these two IMSI codes are identical or correspond with each other. Either they correspond with each other and then the rest of the
35 operation for starting the mobile telephone is permitted (preferably with the

keying in and verification of the PIN code), or these two codes do not correspond with each other and, in this case, the starting operation is not permitted.

However, to allow a genuine possessor of a mobile telephone to change his mobile telephone operator and receive another SIM circuit as a replacement for a previous one, it is preferably planned that if a failure in the comparison of the IMSI codes is observed, then the owner is allowed the possibility of proving that he owns the mobile telephone. This is done simply by then asking him to key in an unit code that is preferably secret. This unit code is preferably different from the IMEI code of the mobile telephone. The keyed-in unit code is then compared with a unit code that is normally stored also in the mobile telephone. If the comparison is successful (indicating that the user is a genuine owner), then the former duplicated IMSI code is modified in the memory of the mobile telephone and replaced by a duplicated IMSI code corresponding to the new SIM card. It is then possible to carry out automatic starting operations as above.

If the comparison is not successful, either the mobile telephone is turned off or, preferably, it is accepted that another attempt can be made to present the unit code, but with a waiting period that increases after each failed attempt.

As an improvement, it is proposed that the duplicated code recorded in the memory of the mobile telephone, especially when this mobile telephone is first put into operation with a new removable SIM circuit, should result from a coupling, in particular by means of an encryption algorithm, between the IMSO subscriber identity code of the SIM card and the IMEI identity code of the mobile telephone, or their equivalent. Preferably, a produced code resulting from this coupling is stored in a non-volatile, rewritable memory of the mobile telephone, for example in an EEPROM or electrically erasable programmable memory. Furthermore, although the invention will be described by taking the IMSI code as the identity code of the removable SIM circuit and the randomly produced IMEI code as the unit code, it could be implemented through the use of other codes, provided that one of them is present both in the removable circuit and in the mobile telephone, even in different forms, and provided that the comparison is made before the mobile telephone is started up.

The invention therefore relates to a method for putting a mobile telephone into service wherein :

- a recording is made, in a removable circuit, connected to the mobile telephone, of a removable circuit identification code,

5 - a utilisation security code is produced in the mobile telephone,

- this utilisation security code of this mobile telephone is recorded in a memory of the mobile telephone,

- when the mobile telephone is put into service, the utilisation security code of this mobile telephone is compared with this removable circuit 10 identification code, and

- the putting into service of the mobile telephone is authorised if this comparison is successful.

characterised in that

- the value of the utilisation security code is compared with a basic 15 code, and

- a new utilisation security code is produced as a function of the removable circuit identification code if this comparison is successful.

The invention will be understood more clearly from the following description and from the appended figures. These figures are given purely 20 by way of an indication and in no way restrict the scope of the invention. Of these figures:

- Figure 1 gives a schematic view of a mobile telephone and its improvement used to implement the method of the invention ;

25 - Figure 2 shows a flow chart that presents the essential steps of the method of the invention.

Figure 1 shows a mobile telephone 1 that can be used to implement the method of the invention. The mobile telephone 1, in a known way, comprises an arithmetic and logic unit 2 connected by a bus 3 to transmission/reception circuits 4. For example, the transmission/reception 30 circuits that can be used in telephony are connected to a loudspeaker 5 and to a microphone 6 and also to a transmission/reception line 7. In order that it may function, the mobile telephone, in a programme memory 8, has a programme 9 as well as a data memory 10. The memory 10 may be the same as the memory 8. Preferably, the memory 10 will be a non-volatile 35 memory, for example of the EEPROM type. Through the bus 3, the unit 2 is

still linked with a connector 11, to which a corresponding connector 12 of a SIM security circuit 13 is connected. The SIM circuit 13 also has an arithmetic and logic unit 14 connected by a bus 15 to a programme memory 16 and to a data memory 17. The data memory 15, in the case of the SIM 5 circuit 13, has the particular feature of being protected against any form of aggression, even against a depassivation of the integrated circuit. The mobile telephone 1 can enter into an RF link 18 with a base station 19 and with central switching circuits 20 of a mobile telephony operator. The central circuits 20 may furthermore be connected to a general switched telephony 10 network 21.

In the prior art, with a keyboard 22 of the mobile telephone 1 connected to the bus 3, a PIN code is keyed in when the telephone 1 is put into service. This PIN code is transmitted by the bus 3 to the SIM circuit 13, in executing an agreed programme in the memory 8 for putting the mobile 15 telephone into service. The arithmetic and logic unit 14 of this SIM circuit 13 then brings about the execution of a programme 23 contained in the memory 16 through which the keyed-in PIN code is compared with a secret code SECRET 24 contained in the memory 17. Should the comparison be successful, the putting into service of the mobile telephone is permitted. This 20 is done especially through the transmission, by means of the connectors 11 and 12, of a piece of IMSI subscriber identity information, herein 25, also contained in the circuits 17 in such a way that this identity information is transmitted by the antenna 7 to the base station 19. After this subscriber information has been processed, the base station 19 allows the mobile 25 telephone to be put into service. More exactly, it incorporates it into its network as a mobile telephone capable, beyond this connection, of entering into communication with another party.

In a known way, as shown schematically in Figure 1, and in a manner comparable to the recording 25 of the IMSI code in the memory 17 of the 30 removable circuit 13, an IMEI code 26 representing the identity of the mobile telephone is recorded in the memory 6 of the mobile telephone 1.

For the codes 25 and 26, it is naturally not obligatory to choose these 35 IMSI and IMEI codes. For example, the circuits of the SIM circuit 13 may comprise serial numbers. These serial numbers may be used especially by the operators, when they wish to incorporate IMSI numbers therein during the

personalising operation, in order to parameterise an encryption machine used to encrypt this IMSI code therein. In every case, whether it is a serial number or an IMSI code itself, it is really an identification code of the removable circuit 13. Similarly the IMEI mobile telephony identification
5 number may be replaced by a serial number produced in one of the integrated circuits connected to the bus 3 and furthermore placed by the manufacturer in the mobile telephone 1.

In the invention, by using at least one of these codes (hereinafter, to simplify the explanation, the IMSI code of the circuit 13 will be chosen) a
10 code called SecretE is produced. This code SecretE is a function of this identification code of the removable circuit. Preferably, a code SecretE is produced by an encryption that is parameterised, for example, by the IMEI identification code of the mobile telephone and possibly other parameters so as to resist systematic unlocking moves. Then, this code SecretE is
15 recorded at a pre-arranged location 27 in the memory 10.

Thus, when the mobile telephone is put into service, the IMSI code stored in the circuit 13 is compared with the code SecretE stored at the location 27. In the event of a successful comparison of course, the mobile telephone is put into service. This comparison is done during a main secrecy
20 sub-programme 28 contained in the memory 8. This secrecy sub-programme 28 essentially compares the contents of the zone 25, possibly encrypted by the contents of the zone 26, with those of the zone 27. In the event of success, this main secrecy sub-programme leads to a main utilisation sub-programme 29 that is comparable in all points to the utilisation programmes
25 known in the prior art. The main sub-programme 29 may comprise especially the request for the keying in of the PIN code by the user.

Since the mobile telephones are provided with the programmes 28 and 29 at the outset when they come off the production line, whereas the circuit 13 is not yet associated with them, it is necessary to produce the code
30 SecretE and store it in the zone 27 when this circuit 13 is effectively associated therewith (without necessarily being connected to it). Figure 2 shows, to this effect, the way in which this marriage operation is preferably conducted by connecting the circuit 13 to the mobile telephone 1. The main secrecy sub-programme 28 gets implemented after an operation of putting
35 the mobile telephone into service : this is typically the switching of a physical

selector switch. It starts with a test 30 to ascertain it is a first-time operation of putting the mobile telephone into service. In the test 30, a comparison is made, for example, between the contents of the zone 27 of the memory 10 and the contents of another zone 31 of the memory 10, which has the same size as the zone 27 and is, for example, contiguous to it. If these two zones 27 and 31 are identical, especially because they have been programmed in the EEPROM 10 identically when the mobile telephone was personalised by the manufacturer, it will be detected that this is a first-time operation for putting the mobile telephone into service. In practice, it is sought to find out if 10 the pre-recorded secret code SecretE is a special code, for example comprising only binary "ones".

If this is the case, the sub-programme 28 is made to perform an instruction 32 in which the SecretE is computed as being a function of the IMSI identification number seen above as well as, if necessary, other numbers such as the serial number of the SIM circuit 13 and/or the mobile telephone 1 and/or the balance of the counter. Once the instruction 32 has been executed and the code SecretE has been produced, an instruction 33 is executed. This instruction 33 essentially comprises the recording of the result of the function, SecretE, in the mobile telephone at the position of the 20 zone 27.

During a first-time operation for putting the telephone into service and executing the instruction 33, it is possible to have this instruction 33 executed either in the circuit 13, in which case the programme 16 of this circuit will have to be arranged accordingly, or preferably in the circuit 2 under the 25 control of the programme 28. It is also possible to obtain the execution of the instruction 33 entirely or partly in the external reader in relation with the circuit 13 and with the mobile telephone 1. Then, once these codes have been delivered, either the telephone is stopped or it is possible to have direct access to the main utilisation sub-program 29.

If this is not a first-time operation for putting the mobile telephone into service, then the contents of the zone 27 are different from those of the zone 31. In the invention, the operation then goes to a test 34 during which the code SecretE recorded in the zone 27 is compared with the IMSI code contained in the zone 25 of the SIM circuit 13. In practice, the verification 35 during a subsequent starting operation comprises the implementation of the

instruction 32 and the comparison of the code produced with the code stored in the zone 27. This comparison is done either by the unit 2 or by the microprocessor 14. Should the test 34 be successful, the use 29 of the mobile telephone is permitted. If the test 34 fails, the user is made to key in
5 the unit code (supposed to represent the IMEI code) and a test 35 is used to ascertain that the keyed-in unit code truly corresponds to the real unit code recorded in the zone 26 of the memory 10. In the event of a failure of the test
10 35, the possibility of another attempt may be prompted by means of an instruction 36. The instruction 36 may include a count of the attempts, a cut-off of the SIM circuit, and/or the setting up of a direct connection of the mobile telephone with a maintenance service of the operator of the circuit 20. It preferably comprises an increasing time lag between each attempt.

A method of this kind works very well since, if the mobile telephone 1 has been stolen, naturally the thief is able to remove only the removable
15 circuit 13, take out a subscription with a mobile telephony operator, replace this removable circuit 13 with another circuit, and try to restart the mobile telephone 1. In this case, the unit code that he launches is a PIN code corresponding to the new circuit 13 that has been communicated to him with his subscription. However, since the programme 28 comprises no test of the
20 PIN code at this stage, there is no likelihood that the keying in of this PIN code will replace the unit code stored in the zone 26. The code that he keys is either a random code, or in the process of being routinely modified. In this case, the increasingly lengthy waiting periods are a discouragement.

However, several situations may arise in this context. Either the legal
25 user may wish to change his operator or he may have lost or forgotten his unit code. When he wishes to change his subscription, he can select an option in the menu to make this change. As an alternative, the proposal to change a subscription leads to a request 36 for keying in the unit code.

If the test 35 is positive, the instructions 32 and 33 are implemented
30 with the production of a new secret code SecretE.

In the other possible situation, if the user has lost his unit code, and especially if he can also prove that he is the legal owner of the mobile telephone, then it can be planned to restore the integrity of this telephone. In this case, the removable circuit 13 is replaced, for example in the services of
35 the mobile telephony operator, by a special removable circuit 37. The circuit

37 is special in that, instead of the information IMSI, its memory 17 comprises a piece of ICCID – Integrated Circuit Card Identification – information that is pre-arranged. Thus, during a test 38, placed for example in the programme 28 before the test 30 and the instruction 32, it will be
5 sought to find out if the subscription number stored in the circuit 13 is a special pre-arranged ICCID subscription number.

For example, the special pre-arranged ICCID subscription number may be furthermore stored in a memory 39 or in an additional zone of the
10 memory 10. In normal times, the test 38 is not successful and the operation goes directly to the test 30. However, if the removable circuit 37 has been positioned in the place of the removable circuit 13, then an instruction 39 is
15 executed, during which the contents of the zone 27 are replaced to make them equal to the contents of the zone 31. The mobile telephone is thus placed again in a state comparable to the one it had when leaving the factory. In this case, it is also possible to launch an instruction 40 during
20 which the unit code is revealed by a screen of the mobile telephone. It is then possible to make the mobile telephone stop. When it is next put into service again, and after a new original removable circuit 13 has been put in, the test 30 then makes the programme jump to the instruction 32 giving rise to the execution of the instruction 33.

Through this procedure, the thief is immediately made to identify himself to the operator and will have to furnish an explanation. Indeed, the
25 ICCID number stored in the memory 39 of the mobile telephone, made available to an operator so that he can sell them to his customers, comprising words of different types, for example ICCID1, whereas those made available to another operator are ICCID2 type words. A first operator will then receive passes 37 comprising special identifications ICCID1 in the memory 17. The other operator will receive passes 37 with another identification ICCID2. In
30 these circumstances, a genuine user will naturally return to his mobile telephone operator to whom he will furnish proof of his subscription (for example with invoices). This operator will naturally introduce the circuit 37 that is suited to the mobile telephone. On the other hand, a thief would go to a wrong operator, will not be furnish the necessary proofs, and will prompt the rejection of the test 38 : the operator will be unable to release the stolen
35 mobile telephone for him.

Thus, a theft becomes useless.

CLAIMS

1. Method for putting a mobile telephone into service wherein
 - a removable circuit identification code (IMSI) is recorded in a removable circuit (SIM) connected to the mobile telephone,
- 5 - a utilisation security code (SecretE) is produced (32) in the mobile telephone,
 - this utilisation security code of this mobile telephone is recorded in a memory of the mobile telephone,
 - when the mobile telephone is put into service, the utilisation security
- 10 code of this mobile telephone is compared with this removable circuit identification code, and
 - the putting into service of the mobile telephone is authorised (29) if this comparison is successful.
characterised in that
- 15 - the value of the utilisation security code is compared with a basic code (11111111), and
 - a new utilisation security code is produced as a function of the removable circuit identification code if this comparison is successful.
- 20 2. Method for putting a mobile telephone into service wherein
 - a removable circuit identification code (IMSI) is recorded in a removable circuit (SIM) connected to the mobile telephone,
 - a utilisation security code (SecretE) is produced (32) in the mobile telephone,
 - this utilisation security code of the mobile telephone is recorded in a
- 25 memory of this mobile telephone,
 - when the mobile telephone is put into service, the utilisation security code of this mobile telephone is compared with this removable circuit identification code, and
 - the putting into service of the mobile telephone is authorised (29) if this comparison is successful.
characterised in that
 - the value of the identification code of the removable circuit is compared with a code listed in a list of codes listed and recorded in the mobile telephone, and in the event of success,
- 30 35 - the value of the utilisation security code recorded in the mobile

telephone is made to be equal to a basic value (11111111), or

- the putting into service of the mobile telephone is authorised, or
- a code is communicated for unlocking the use of the mobile telephone.

5

3. Method for putting a mobile telephone into service wherein

- a removable circuit identification code (IMSI) is recorded in a removable circuit (SIM) connected to the mobile telephone,

- a utilisation security code (SecretE) is produced (32) in the mobile telephone,

10

- this utilisation security code of this mobile telephone is recorded in a memory of the mobile telephone,

- when the mobile telephone is put into service, the utilisation security code of this mobile telephone is compared with this removable circuit identification code, and

15

- the putting into service of the mobile telephone is authorised (29) if this comparison is successful,

characterised in that

- in the event of failure of the comparison, when the telephone is being put into service, between the utilisation security code of this mobile telephone

20

and this removable circuit identification code,

- a request is made for the keying in of an unlocking code, and

- a new utilisation security code (SecretE) of this mobile telephone is recorded in the memory of the mobile telephone, this new utilisation security code corresponding to the identification code of the removable circuit present at this time in the mobile telephone.

25

4. Method according to one of the claims 1 to 3, characterised in that

- the utilisation security code is encrypted before it is recorded, in encrypted form, in the memory of the mobile telephone.

5. Method according to one of the claims 1 to 4, characterised in that

30

- as a removable circuit identification code, a subscriber code to a mobile telephony service is used.

6. Method according to one of the claims 1 to 5, characterised in that

35

- an unlocking key is produced at the time of producing the security code (SecretE) as a function of the identification code of the mobile telephone and of the identification code of the removable circuit, and

- this unlocking key is presented.

7. Method according to one of the claims 1 to 6, characterised in that the utilisation security code is a function of the identification code of the removable circuit and of a mobile telephone identification code (IMEI).

5 8. Method for putting a mobile telephone into service substantially as hereinbefore described with reference to the drawings.



Application No: GB 0018673.4
Claims searched: 1

14

Examiner: Gareth Griffiths
Date of search: 21 February 2001

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.S): H4L (LEF)

Int Cl (Ed.7): H04Q 7/32, 7/38

Other: Online Databases: WPI, EPODOC, JAPIO

Documents considered to be relevant:

Category	Identity of document and relevant passage	Relevant to claims
A	GB2335568 A (NEC) whole document	
A	GB2285559 A (MOTOROLA) p.3 line 4 - p.8 line 22	
A	EP0607767 A1 (ERICSSON) whole document	
A	WO97/43866 A2 (ERICSSON whole document	

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.